Page 2279 - 2304 **DOI:** *https://doij.org/10.10000/IJLMH.111561*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 4 | Issue 4

2021

Right to Privacy, Social Security and State Powers - The Orwellian State: Fiction or Fact?

SANIKA KADAM[1] AND SHEETAL KIRI[2]

ABSTRACT

Every second that we are on the internet, our digital footprint is exchanged, processed and stored in one form or another. The obvious questions raised here are- What happens to the data? How is it used? Who controls the way it is collected, processed and stored? Is the data weaponized in any way? What is the role of the State in this? What mass surveillance techniques are employed by the State, if it is in place? What are our rights in this? The aim of the research paper is to thoroughly investigate and try to answer the questions raised above. The paper also delves into the history of the concept of privacy and data protection whilst taking into account the events that have happened in the past or are unfolding presently, contributing to the global debate of personal data privacy and have led to the development of some comprehensive legislations in EU and India to tackle the same.

Keywords: *Ads, data, Facebook, interception, mass surveillance, personal data, privacy, State.*

I. INTRODUCTION

The functions and powers of a state have undergone a drastic change; in the 21st century a modern state's nature and functions have advanced owing to the ever growing technological advancements. Today, security of one's country and its people is of prime importance. With the rise in extremist activities, terrorism, crime, civil wars and social unrest in a modern state and the threat that these impose upon smooth functioning of a state; it is considered justifiable to snoop on citizens in the pretext of national security. Surveillance or snooping by the state on its citizens can be done through various ways like physical surveillance, phone tapping and electronic surveillance. However, surveillance today is much more penetrative than what it was in the past.

[1] Author is a LLM student at Symbiosis Law School, Pune, India.
[2] Author is a LLM student at Symbiosis Law School, Pune, India.

 [ISSN 2581-5369]

In 1948, an English writer published a book called 1984, which was a story set in a dystopian society where a character called Big Brother had access to all the data about a person, their every move, and thought through huge screens installed everywhere. This book started retting a cult status as the once fictional dystopia started taking a form of reality. Surveillance or 'spying' by the state is not something new, in-fact it dates back to the colonial rule in India when the British security forces conducted surveillance to keep a check on dissenters. Even after India's independence, democratic governments have conducted various kinds of surveillance on its citizens. In the modern world, new forms of surveillance have come into the picture due to the internet and technological advancements. Some instances of spying in the modern state can be that of the increasing powers of the intelligence agencies and their services, collection and storage of data of individuals by the government and also buying such data from private actors. While technology penetration in personal lives is on the increase the laws are not at the same pace to secure the citizen's rights and freedoms. This seems a little problematic and concerns of privacy violations in a democratic state can be raised.

II. CONCEPT OF THE RIGHT TO PRIVACY

Privacy essentially means, one's right to determine the extent to which he wishes to share his personal information with others. It is living one's life as one desires without any interference. Protection of privacy is often seen as a way in which a line can be drawn at how far a society can penetrate into one's personal affairs.[3] Concept of privacy has also evolved from the primitive times where intrusions were only limited to trespassing, eavesdropping etc. But in the modern age, privacy intrusions have increased exponentially with the advent of technology. We have telephone wiretaps for overhearing, spycams for undercover intelligence operations, computers, mass storage devices for collecting, storing and circulating personal and financial information. Privacy violations can include, interception and storage of digital information, profiling of marginalized groups, biometric data dangers, censorship and surveillance by private actors that collect our information.[4]

Right to Privacy is considered a fundamental human right and has been talked about in various international conventions and treaties. It has also been imbibed in constitutions of various countries. The Universal Declaration of Human Rights talks about privacy in Article 12[5], "No

[3] Ashok Kumar Kasaudhan, *Surveillance and right to privacy: Issues and challenges*, Vol. 3, INT. JOURNAL OF LAW 73, 74 (2017)

[4] Dr. Keith Goldstein, Dr. Ohad Shem Tov & Mr. Dan Prazeres, *Right to Privacy in the Digital Age*, OHCHR (April 9, 2018) https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/PirateParties International.pdf.

[5] Universal Declaration of Human Rights, 1948, Art. 12.

 [ISSN 2581-5369]

one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." Likewise, Article 17 of the International Covenant on Civil and Political Rights talks about no arbitrary interference with one's privacy and protection from law against such attacks.[6] Article 8[7] of European Convention on Human Rights talks about the right to respect for private and family life, prohibiting any interference by public authority except in exceptional circumstances where concerns of "national security" etc. are at stake.

III. RIGHT TO PRIVACY IN INDIA

Right to privacy has no explicit mention in the Indian Constitution. However, the courts have interpreted Article 21[8] of the Indian Constitution "Right to life and personal liberty" to include it within its ambit. The landmark judgement which asserted Right to Privacy as a fundamental right was the case of Justice K.S. Puttaswamy and ors. V. Union of India (2017)[9]. Before the Puttaswamy judgement, the 1954 judgement in the case of M.P. Sharma[10] and the 1962 judgement in the case of Kharak Singh[11] held that privacy is not a fundamental right. In the latter, the court recognised the common law right to privacy[12] but said it wasn't guaranteed by the constitution and held the 'domiciliary visits' done by the UP police as 'unconstitutional', striking down the provision allowing it.

In the case of People's Union for Civil Liberties (PUCL) v. Union of India, (1997)[13], the SC elevated privacy rights in India and held it to be a part of Article 21. The case primarily dealt with the issue of telephone tapping. They held that privacy can only be infringed in grave circumstances of public emergency and only according to the 'procedure established by law'. The Supreme Court further issued guidelines for the issuance of telephone tapping orders to regulate such actions and put a check on arbitrary administrative actions[14]. Pior to the said case there were no guidelines for telephone tapping cases and there was also no law in place to

[6] International Covenant on Civil and Political Rights, 1966, Art. 17.
[7] European Convention on Human Rights, 1953, Art. 8.
[8] INDIA CONST., Art. 21.
[9] Justice K.S. Puttaswamy and ors. V. Union of India, (2017) 10 SCC 1.
[10] MP Sharma v. Satish Chandra, AIR 1954 SC 300.
[11] Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295.
[12] Priyanka Mittal, *Is privacy a fundamental right? Two cases that SC will look at*, LIVEMINT, (19 July 2017), https://www.livemint.com/Politics/7oHGx6UJfLD0uIDXFwV9CL/Is-privacy-a-fundamental-right-Two-cases-that-Supreme-Court.html
[13] People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301.
[14] Bharat Vasani et al, Right to Privacy: Surveillance in the post-Puttaswamy Era, BLOOMBERG QUINT, (12 November 2019) https://www.bloombergquint.com/law-and-policy/right-to-privacy-surveillance-in-the-post-puttaswamy-era

 [ISSN 2581-5369]

check the surveillance done by the government. After the PUCL case, the guidelines were codified in Rule 419(A)[15] of the Indian Telegraph Rules, 1951 in 2007.

In the case of Justice K.S. Puttaswamy and ors. V. Union of India (2017)[16], the question regarding the constitutionality of the 'Aadhaar System' was raised. One integral issue was whether the biometric data collected by the Government violated privacy. To answer this question, SC first tried to establish if there was a privacy right in India. The court held that the right to privacy was intrinsic to Article 21 of the Constitution and also the freedoms guaranteed by part III of the constitution like Article 14 and 19. They went on to overrule the judgements in Kharak Singh and MP Sharma to the extent they held otherwise. Further, the court set out a 'proportionality' test in case of privacy intrusion by the state. It held that the action must be sanctioned by law; legitimate objective for action must be there; there must be proportionality in the action and need for interference; and that power to interfere must adhere to procedural guarantees. This case is of utmost significance if we talk about privacy rights in India as it established privacy as a fundamental right and granted protection to the same.

IV. RIGHT TO PRIVACY VS. RIGHT TO INTERCEPT

Privacy right is not absolute was ruled in the Puttaswamy case of 2017[17]. The right is not unbridled and can be over stepped upon in case of a public emergency or in the larger interest of public safety; without which it would not be lawful for the state to conduct interception or surveillance on an individual. Just as 'reasonable restrictions' can be imposed on other fundamental rights and freedoms, the same applies to privacy rights aswell. With the rise in technology digital communications have increased and thus in today's time this interception by state focuses primarily on the digital realm. However, if surveillance is not lawful then the state is acting in excess of its powers and can be termed no less than a 'Surveillance State' which absolutely undermines a democracy.

Right to intercept would mean state's right to "receive a communication or signal directed elsewhere usually secretly[18]" for matters of national interest. When the state has reasonable grounds and evidence they can conduct interception of individuals, lawfully. It is permissible in India and various sections afford this right to the state. However, there is always a tussle between right to privacy and right to interception. But in today's age and time, with the rise of terrorism (including cyber terrorism), fake news, hate speech leading to riots and other illegal

[15] Indian Telegraph Rules, 1951, Rule 419-A.
[16] Justice K.S. Puttaswamy and ors. V. Union of India (2017) 10 SCC 1.
[17] Ibid.
[18] Merriam-Webster Dictionary https://www.merriamwebster.com/dictionary/intercept

activities the importance of interception by state cannot be subverted. To uphold and maintain privacy rights it is significant to note that such powers of interception cannot be invoked by the government in an arbitrary or unreasonable manner. In the case of Vinit Kumar vs. Central Bureau of Investigation Economic Offences Division (2019)[19], the Bombay HC ruled that an order for interception cannot be made to target specific persons for economic offences and cannot be misused arbitrarily. Further after an appeal was made in SC, the SC held that economic emergency cannot fall under 'public emergency' and thus economic offences does not call for interception and would not be permissible under law. Thus, this judgement clearly states that if something does not fall under 'public emergency' or public safety' threshold[20] then surveillance by state cannot take place and such interception would be unlawful. The same principle would apply to cases of unlawful interception in cyberspace too.

The PUCL decision of 1997 laid guidelines to check executive's surveillance powers and for the proper use of this power. It laid 5 grounds for issuance of interception order along with the mandatory obligation to issue such orders only on grounds of public emergency-

1. Competent authority who can issue such order i.e. Home Secretary
2. Review of such an order must be sent to the Review Committee within one week,
3. Duration of validity of the order i.e. two month's
4. Destruction of such intercepted communications when they were no longer necessary
5. Records of intercepted communication, the amount of disclosure of such material, identity and number of people to whom it is disclosed, how much intercepted material is copied and the no. of such copies should be maintained by the intercepting authority.

This case paved the way for the codification of these guidelines by Rule 419-A of the Indian Telegraph Rules, 1951. The PUCL guidelines[21] would apply to interception orders of digital surveillance too which is mandated by the Information Technology Act (IT Act), 2000. The Information Technology Rules, 2009 lay down procedural guidelines for data surveillance conducted under Section 69 of the IT Act, 2000 and are quite similar to provisions under Rule 419-A of telegraph rules.

V. LAWS RELATING TO MASS SURVEILLANCE IN INDIA

Laws that regulate surveillance in India can be invoked on certain exceptional and necessary

[19] Vinit Kumar vs. Central Bureau of Investigation Economic Offences Division WP No. 2637 of 2019.
[20] Bharat Vasani et al, *Surveillance in the post-Puttaswamy Era*, MONDAQ, (19 November 2019), https://www.mondaq.com/india/privacy-protection/865282/surveillance-in-the-post-puttaswamy-era
[21] People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301

 [ISSN 2581-5369]

circumstances only. For surveillance to be valid and lawful it must be done within the legal framework and boundaries only. The Indian Telegraph Act regulates the law relating to telephonic surveillance. Section 5(2)[22] permits 'telegraph' lines surveillance on the necessary grounds of 'public emergency' or for 'public safety'. After the PUCL case the procedural guidelines given in the case were codified in Rule 419A[23] of the Indian Telegraph Rules, 1951 to keep a check on arbitrary surveillance and provide a lawful procedure to the same.

The Information Technology Act deals with Internet surveillance in India. Section 69[24] of the Act mandates the government of Center and States to "issue directions for interception or monitoring or decryption of any information through any computer resource" if they are satisfied about it's necessity "in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence."

Section 69 of the IT Act has two additional grounds as compared to Section 5(2) of the Telegraph Act, they are, 'defence of India' and 'investigation of any offence' for the invocation of the interception orders. Section 69B of the IT Act talks about the Government's power to collect and monitor 'traffic data' from any computer resource. 'Traffic data' would mean data that provides information on "communications origin, destination, route, time, data, size, duration or type of underlying service or any other information." Collection of 'traffic data' or metadata is important as it gives information about basic data.

VI. AUTHORITIES WORKING UNDER INDIAN GOVERNMENT FOR SURVEILLANCE

The Ministry of Home Affairs order dated 20.12.2018[25] authorised 10 security and intelligence agencies to intercept and monitor electronic communication and information under section 69 of the IT Act, 2000 and Rule 4 of IT Rules, 2009. These agencies were Narcotics Control Bureau, Intelligence Bureau, Central Board of Direct taxes, National Investigation Agency, Enforcement Directorate, RAW, Commissioner of Delhi Police, Directorate of Revenue Intelligence, Directorate of Signal Intelligence and Central Bureau of Investigation. Various criticisms were targeted at the government after the said order by the public and opposition leaders. They were accused of creating a Surveillance State. The government then issued a

[22] Indian telegraph Act, 1885, Section 5(2)
[23] Indian Telegraph Rules, 1951, Rule 419-A
[24] Information Technology Act, 2000, No. 21, Acts of Parliament 2000 (India).
[25] Ministry of Home affairs, S.O. 6227(E) http://egazette.nic.in/WriteReadData/2018/194066.pdf

 [ISSN 2581-5369]

press release[26]to bring clarity. They clarified that new powers have not been bestowed on these agencies and that these agencies cannot voluntarily intercept information. It was further clarified that no powers have been delegated to these agencies and only on the order of the Union Home secretary can these agencies proceed to intercept, decrypt and monitor. This solution has been taken up by various governments to counter terrorism, cyber terrorism and for state security at large. Such surveillance in cyberspace can be done by tracking cell phones, emails, messages (including messages on facebook and whatsapp), social media platforms etc. Some bodies set up by the government for the purpose of surveillance are discussed hereunder.

1. National Intelligence Grid (NATGRID)[27] came into existence post 26/11 attacks in 2009, to keep a check on crime and terror threats faced by the country. Its main aim is to formulate a centralised database that all intelligence agencies can access. The centralised database will collect information from various government databases such as railway and airline tickets, visa and immigration records, tax, credit and debit cards, telecom, driving licenses etc. the intelligence agencies such as Narcotics Control Bureau, Research & Wing Analysis, Enforcement Directorate can access such information to tackle the problem of terror and crime.

2. The Central Monitoring System (CMS) aims to surveil telecommunications and monitors phone calls, text messages, activities online and on social media etc. This was also initiated in 2009 to strengthen India's security structure[28]. Prior to CMS the government had to contact middlemen for the purpose of interception like the telecom service providers when they had the suspect of criminal or terror activities. CMS enables the government to target the suspect directly via a central system.

3. Network Traffic Analysis (NETRA) is a surveillance tool to monitor internet traffic. They use pre-defined filters such as keywords like 'murder', 'bomb', 'terrorist', 'attack'[29] etc and identifies the IP address of the sender and notifies the intelligence authorities when they fear there is a potential threat to security. Research & Wing Analysis that deals with external intelligence, Cabinet Secretariat and Intelligence Bureau are three agencies that NETRA serves.

[26] Ministry of Home affairs, PIB Delhi https://pib.gov.in/PressReleseDetail.aspx?PRID=1556945

[27] Ashok Kumar Kasaudhan, *Surveillance and right to privacy: Issues and challenges*, Vol. 3, INT. JOURNAL OF LAW 73, 75 (2017).

[28]*Watch the watchman series Part 2: Centralised Monitoring System*, INTERNET FREEDOM FOUNDATION, (14 September 2020) https://internetfreedom.in/watch-the-watchmen-series-part-2-the-centralised-monitoring-system/

[29]*NETRA: A vigilant eye on the internet*, RESEARCH MATTERS, (8 March 2017) https://researchmatters.in/article/netra-vigilant-eye-internet

 [ISSN 2581-5369]

4. Unique Identification Authority of India (UID Scheme) and National Counter Terrorism Center[30] (NCTC) are the other two monitoring systems. While the former is unique because it contains biometric, iris scan etc of all citizens of the country. NCTC was proposed to fight terrorism post 26/11 attacks to strengthen the security and surveillance framework in the country.

VII. MASS SURVEILLANCE IN CHINA

In China, Orwellian state is a reality. The surveillance and censorship conducted by the government in China is chilling. China monitors its citizens through cameras, physical surveillance by deploying military forces in the sensitive areas where various ethnic groups reside to prevent the repetition of the uprising like the one seen in 2009 by the Uyghur Muslims and of course the internet censorship.

The Great Firewall of China[31] is the nickname given to the collective methods used by the government including technology and policies to control and monitor the activities on the internet. The various tools adopted by the government that sum up to be the firewall block foreign websites access, apps etc, censors the content that circulates on the internet and removes content that is prohibited. It is viewed by China as "Internet sovereignty"[32], that means they as a country should be able to decide what and how the internet should function in their country. It enables a virtual blockage from the outside world; sites such as Google, Instagram, Facebook are all banned in China. Instead of google there is a domestic search engine called Baidu which is heavily censored and shows only what the government wants people to see.

The firewall censorship is done by using methods like DNS poisoning, Blocking VPNs, Blocking IPs, Filtering URLs[33] which prevent people from using blocked sites and servers. Deep Packet Inspection[34] technology is used to block servers, sensitive content and sites by detecting keywords. Chinese government can't even take a joke or a slight dissent; when Chinese President Xijinping was compared to Winnie the Pooh (Such comparison was first made in 2013 when picture of Barack Obama and Xi was compared as striking resemblance to

[30] Ashok Kumar Kasaudhan, *Surveillance and right to privacy: Issues and challenges*, Vol. 3, INT. JOURNAL OF LAW 73, 75 (2017).
[31] Paul Mozur, Baidu and Cloudfare Boost Users over China's Great Firewall, NYTIMES, (13 September 2015) https://www.nytimes.com/2015/09/14/business/partnership-boosts-users-over-chinas-great-firewall.html
[32] Simon Denyer, China's scary lesson to the world: Censoring the Internet works, WASHINGTON POST, (23 May 2016), https://www.washingtonpost.com/world/asia_pacific/chinas-scary-lesson-to-the-world-censoring-the-internet-works/2016/05/23/413afe78-fff3-11e5-8bb1-f124a43f84dc_story.html
[33] Chris Hoffman, How the "Great Firewall of China" works to censor China's Internet, HOW-TO GEEK, (10 September, 2017) https://www.howtogeek.com/162092/htg-explains-how-the-great-firewall-of-china-works/.
[34] Chris Brook, What is Deep Packet Inspection? How it works, Uses cases for DPI, and more, DIGITAL GUARDIAN, (5 December 2018) https://digitalguardian.com/blog/what-deep-packet-inspection-how-it-works-use-cases-dpi-and-more.

 [ISSN 2581-5369]

pooh and Tigger[35] then a plethora of memes were shared online regarding such comparison of Xi with Pooh. The government started censoring and erasing these memes from the internet. A photo of Xi compared to Pooh during a military parade was the most censored image in 2015.

Skynet[36] is China's video surveillance network for "live surveillance and recording". They even introduced facial recognition technology[37], there are cameras in every public space to keep a check on threats, crimes etc. It is even used to single out minority communities and keep a special tab on them like the Uyghurs, the government uses propaganda, surveillance and re-education camps to try to bring Uyghurs and similar communities in line with the Communist party's ideology and lines. There are more than 200 million surveillance in the whole country used to monitor citizens, amounting to one camera for seven citizens[38]. All of this is used to curb political dissent and social unrest even before it takes place and that people obey laws and don't question their policies.

The Social Credit System is the newest introduction to methods of surveillance in China. It was first announced in 2014 and was launched at provincial level for testing with their individual pilot systems. The nationwide uniform system is soon to be launched. According to this system, all citizens and businesses will be assigned a 'Social Credit score' that will increase or decrease according to their actions. Actions that are socially beneficial will lead to increase in score and socially harmful actions will lead to decrease in score and people with high scores will get multiple benefits and those with low scores will get punishments. Different provinces have now adopted different criteria for good and bad behaviour, some actions that would amount to good behaviour are donating blood, paying bills on time, abiding by traffic rules etc. spreading fake news, dissent and protest against government, not sorting waste properly etc. would amount to bad behaviour. Good credit score would amount to benefits such as priority admissions in universities, tax breaks and incentives, lower waiting time in hospitals etc.; bad credit score would lead to punishments such as low speed internet, ban from public transports such as flights and trains. According to Channel News Asia, nine million people were not allowed to buy flight tickets due to low credit scores. According to Beijing News, the government barred 17 people from enrolling in higher education because they refused to do

[35] Benjamin Haas, China bans Winnie the Pooh film after comparisons to President Xi, THE GUARDIAN, (7 August 2018) https://www.theguardian.com/world/2018/aug/07/china-bans-winnie-the-pooh-film-to-stop-comparisons-to-president-xi

[36] Thomas J Ackermann, What is china's SKYNET (yes: it is what you think it is), BGP4, (10 May 2019) https://www.bgp4.com/2019/05/10/what-is-chinas-skynet-yes-it-is-what-you-think-it-is/

[37] Alfred Ng, How China uses facial recognition to control human behaviour, CNET, (11 August 2020) https://www.cnet.com/news/in-china-facial-recognition-public-shaming-and-control-go-hand-in-hand/

[38] Paul Mozur, Inside China's Dystopian Dreams: AI, Shame and Lots of cameras, NY TIMES, (8 July 2018) https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html

 [ISSN 2581-5369]

military service. All these are just some examples of the Chinese government controlling the lives and actions of their citizens. In China, Orwellian state is a reality, where government censorship and propaganda curb the freedoms of the citizens and dictate upon what is permissible and what is not[39].

VIII. MASS SURVEILLANCE IN THE USA

Post the 9/11 attacks in 2001, the United States expanded its surveillance and intelligence capabilities to keep a check on terror and for its security concerns. Subsequently the Patriot Act was passed in October to counter terrorism and expand the state's power to surveil. The FISA Act was amended in 2008; Section 702 gives vast powers to the intelligence authorities and authorises the state to monitor their citizens phone calls, emails and all activities on the internet for a week without a warrant.[40]

The Executive Order 12333 was passed to extend the US intelligence agency's powers and authorises the state to conduct surveillance to collect 'foreign intelligence', however since there is no judicial check on the same various 'backdoor searches' of the US nationals are conducted even for domestic investigations which have no connection with foreign intelligence. Both these sections give wide powers to the state to sweep personal communications of their nationals and thus should be narrowed down and the role of Foreign Intelligence Surveillance Court should be expanded to conduct targeted surveillance based on probable cause as opposed to the current role of 'annual review of general targeting'[41] as mandated by section 702.

Edward Snowden in 2013 revealed the PRISM program through which the government collected a vast amount of call records of their citizens and internet communications with the help of internet companies such as Google, apple etc[42]. The US Privacy Act of 1974 was passed to prevent misuse of personal data of the citizens and created rights such as data minimization, access to one's personal data held by the government etc. however it does not apply to data collected by internet companies. There are consumer privacy acts such as Children's Online Privacy Protection Act[43] which protects children's data under 13 years of age by entities and

[39] Alexandra Ma, China ranks citizens with a social credit system- Here's what you can do wrong and how you can be punished, INDEPENDANT, (8 May 2018), https://www.independent.co.uk/life-style/gadgets-and-tech/china-social-credit-system-punishments-rewards-explained-a8297486.html

[40] Ashley Gorski et al, The future of US Foreign Intelligence Surveillance, JUST SECURITY, (11 November, 2020) https://www.justsecurity.org/73321/the-future-of-u-s-foreign-intelligence-surveillance/

[41] Ibid.

[42] Bill Chappell, NSA Reportedly Mines servers of US Internet firms for data, NPR, (6 June 2013) https://www.npr.org/sections/thetwo-way/2013/06/06/189321612/nsa-reportedly-mines-servers-of-u-s-internet-firms-for-data

[43] Children's Online Privacy Protection Act, 1998, 15 U.S.C. §§ 6501-6505.

persons based in US; Gramm-Leach-Bliley Act[44] regulates financial institution's dealings of citizens private information; and Health Insurance Portability and Accountability Act[45] stipulates data confidentiality related to healthcare by healthcare insurance industries. Understanding the importance of privacy protection certain states like Maine, California and Nevada[46] have effectuated their own privacy laws which give comprehensive protection to the citizens of their states and several other states like Newyork, Maryland etc. have proposed the same but the acts are yet to be passed. It is to be noted that there is no federal level consumer protection data yet in the US like the GDPR.

IX. PERSONALIZED ADVERTISEMENT MODELS AND DEMOCRACY

The main purpose of the internet, when it was developed for the military, was to enable the exchange of security and defence related data over long distances in an efficient, lightning speed effectively.[47] When it was opened to access for the common public, it enabled people to communicate with their friends and families on a regular basis. Therefore we can say that social media has been around for as long as the internet in various forms. Initially it was chatrooms, forums, emails, instant messaging clients etc. In 2004, came Orkut and Facebook, almost simultaneously, which were the precursors to all the social media platforms available now- a consolidated list of contacts, features to add and share pictures, videos, scrapbook/ wall where people could leave their messages, forums, communities, groups, etc. It revolutionized the way strangers communicated. Instead of communicating with one's pen pal, say, Romania through snail mail, people just added that person as a contact on their social media account and built a real connection. Facebook's popularity remained contained initially since one required an institutional email address to sign up. Also, it was an exclusive, invitation-only party amongst the universities in the USA.

2006 marked the beginning of a global social experiment. The micro-blogging site, Twitter, came up where you had to express your thoughts in 140 characters or less. Facebook opened up for everyone to sign up, although Orkut was way ahead in terms of popularity. It was then that Facebook introduced various games, that are now recognised by the psychologists as clickbaits- a title or picture so irresistible to the human brain that clicking on it becomes almost an instinctual response. These games, for the exchange of your data and a personalised quick

[44] Gramm-Leach-Bliley Act, 1999, 15 U.S.C. §§ 6801-6809.
[45] Health Insurance Portability and Accountability Act, 1996, 5 U.S.C.
[46] Andy Green, Complete Guide to privacy Laws in the US, VARONIS, (29 March 2020) https://www.varonis.com/blog/us-privacy-laws/
[47] Evans Andrews, *Who Invented the Internet?*, HISTORY, (Oct 28, 2019), https://www.history.com/news/who-invented-the-internet/.

response based questionnaire, gave the user their personality traits, or what character traits of a famous movie, etc they have. These fun, seemingly harmless games and the data that they harvested would have catastrophic consequences, which would then become a public knowledge and a raging controversy a decade later, for having manipulated the Presidential elections of a country that considered itself the champion of liberty and democracy. But before that, came the monetization of the internet.

While corporates always advertised on the internet in some form or the other, in 2007 Facebook introduced Facebook Ads[48] and in 2010 Twitter jumped on the ads bandwagon[49]. It was a revenue model where corporations could target advertisements to specific users based on the data that Facebook had harvested on each of it's users. Simply put, if a young woman in her 20s, who had recently updated that she works in some XYZ company (meaning she had become an independent salaried person with a disposable income) had liked the page of an apparels company, say Zara, she would get suggestions and ads of other apparel, jewelry, handbag, and lifestyle companies in affiliate marketing. In the beginning, these ads were random. But over the time the algorithms suggesting these ads have become so eerily specific that there's an ongoing joke amongst the heavy internet users that if they even dream about a particular thing, the next morning an ad about that thing pops up in their feed. It was the introduction of "like", "retweet", "share", "comment" buttons on Facebook, Twitter around 2010 that marked the decline of Orkut, which eventually shut down its operations in 2014.

The personalised ads story started taking a crucial turn in 2010, almost simultaneously, when primitive smartphones were launched. The introduction of a Facebook mobile app for iOS in 2008, for Android and Blackberry devices in 2010[50], and that of microphone and virtual, voice commands based digital assistant in 2011[51], as well as the live tracking GPS embedded in the smartphones, the internet giants had an intimate access to our daily lives, habits, behaviours, in essence the emotional pulse of the user.

The question of how all these factors add up to the manipulation of mandate in elections can now be understood in the following instances.

[48] *Facebook Unveils Facebook Ads*, FACEBOOK, (Nov 6, 2007), https://about.fb.com/news/2007/11/facebook-unveils-facebook-ads/.

[49] Josh Constine, *Twitter Ads Are Finally Available To All US Businesses, No Longer Invite Only*, TECH CRUNCH, (Apr 30, 2013), https://techcrunch.com/2013/04/30/twitter-ads-available/.

[50] Mansoor Iqbal, *Facebook Revenue and Usage Statistics (2020)*, BUSINESS OF APPS, (Oct 30, 2020), https://www.businessofapps.com/data/facebook-statistics/

[51] Phil Gray, *The Rise of Intelligent Virtual Assistants*, INTERACTIONS, (Jun 1, 2016), https://www.interactions.com/blog/intelligent-virtual-assistant/rise-intelligent-virtual-assistants/

 [ISSN 2581-5369]

X. DISINFORMATION AND THE ALGORITHM BIAS

The availability of various platforms at one's fingertips gave the social media users the opportunity to voice their opinions- political or otherwise, and to gain traction amongst like-minded people and command a clout of followers. Rumour-mongering and spread of incorrect information has been around for as long as humankind. While the internet ensured that these pieces of misinformation spread at a faster speed, the social media amplified its effect a hundred-fold. Many times such misinformation came from a political figure or a person with a huge following and credibility. Due to the lack of fact-checking agencies, these pieces of misinformation turned into fervent political propaganda and received a wide circulation. This is termed as "information bias" in psychology- people tend to believe the information that supports their personal opinion.

These trends have led to the emergence of a new term- disinformation. It means that a piece of false or misleading information that is planted and spread covertly and deliberately with the intention of influencing the public perception and opinion.

At the same time, it has been observed that the algorithms used on these platforms develop a bias in favour of extremist ideologies. In essence, a person will be automatically recommended the content which is divisive and extremist in nature, leaning towards right-wing or left-wing- whatever is the person's natural leaning as profiled by the algorithm. The creators of these algorithms are themselves astounded and clueless about how the algorithms evolved in this manner[52].

XI. CAMBRIDGE ANALYTICA

CA was a political consulting firm founded in 2013 by Alexander Nix, specialising in political campaigns for elections. They reportedly purchased the personal data of 87 million users from the various defunct Facebook games, who had retained the personal data of the users long after the closure, to create a profile and political preference of each user. At its peak, CA had upto 5000 data points on each of its profiled Facebook users. Based on this personal profiling, voters who were yet undecided and leaning towards a particular candidate were targeted for advertising of the candidate. The constant hammering of a particular political ideology and a candidate, combined with the rampant disinformation led to successful conversion of mandate. This firm came into the limelight in March 2018 through a whistleblower, an ex employee of CA, Christopher Wylie. CA was employed by various political parties around the world, most

[52] Jonathan Haidt & Tobias Rose-Stockwell, *Social Media is Warping Democracy*, THE ATLANTIC, (Dec 2109), https://www.theatlantic.com/magazine/archive/2019/12/social-media-democracy/600763/

 [ISSN 2581-5369]

scandalously, by the 45th President of US, Donald Trump, in order to manipulate the mandate and outcome of the Presidential elections, infamously known as Project Alamo. At its peak, Project Alamo was spending $ 1 Million/day on Facebook ads[53].

There have been claims that CA was employed by the groups in favour of Britain leaving European Union ahead of the Brexit referendum, however, this remains to be investigated by the authorised law enforcement agencies[54].

XII. ANKHI DAS AND THE RIGHT WING BIAS

Ankhi Das was the Policy Head of Facebook Inc. India for 10 years before quitting in October 2020. She came into headlines when the Wall Street Journal implicated her in some serious hate-speech related allegations. Allegedly, it was she who decided not to the anti-Muslim delete posts reported by the users as hate speech, since the person making the posts was an eminent legislator from the ruling party in India, a Hindu nationalist regime- Bharatiya Janta Party.

Ms. Das has also been accused of favoring pro-BJP content whilst aggressively flagging and removing the content not in favour of BJP. There have been reports that she took no action against hate speeches and disinformation by pro-BJP users and pages, thus violating Facebook's own Community Guidelines. Facebook India has come under scrutiny for influencing 2014 and 2019 general elections via heavy political advertising on the platform, where BJP reportedly spent a fortune on the social media campaign[55].

This instance provides a foundation for the claim that algorithms are not all-powerful and that human intervention and biases do play a crucial role in the social media infrastructure.

XIII. EVENTS THAT TRIGGERED MASS SURVEILLANCE

It should not come as a surprise that the internet is used for mass surveillance, given that it was basically developed in the 1960s for the US Department of Defence with the intention of surveillance and speedy communication in case of nuclear attacks by the USSR in the Cold War era. It is also a fact that governments around the world- monarchies, authoritarian regimes, dictatorships, democracies, or communist regimes- are all bound by a common thread, namely, the desire to have access to the coveted common population's personal information and

[53] Julia Carrie Wong, *The Cambridge Analytica Scandal Changed the World- but it Didn't Change Facebook*, THE GUARDIAN, (Mar 18, 2019), https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook

[54] Ibid.

[55] Newley Purnell & Jeff Horwitz, *Facebook's Hate-Speech Rules Collide With Indian Politics*, THE WALL STREET JOURNAL, (Aug 14, 2020), https://www.wsj.com/articles/facebook-hate-speech-india-politics-muslim-hindu-modi-zuckerberg-11597423346.

communication, albeit to a varying degree. Certain events were so catastrophic that it provided the Governments a legitimate ground for surveillance. Some of these are the 9/11 Twin Tower attacks in the US, 26/11 Taj terror attacks in Mumbai, India, various terror attacks all over Europe, most notably London tube, hate crimes and the rise of extremist groups are the examples to name a few.

However, it was due to the Arab Spring in 2010 that drew attention of the Governments towards the possibility of a regime being toppled by a leaderless but coordinated mass movement facilitated by the Internet.

XIV. SOCIAL MEDIA AND THE REVOLUTIONS

With the advent of social media, it was probably for the first time in the history of mankind that organising movements and protests became so easy, cost effective and efficient. It was a matter of simply creating an event on Facebook or amplifying the tweet with thousands of retweets and trending hashtags and a few hundred people at the least will show up at the venue. Coordination became easier too since it has become possible to hold protests in various cities at the same time for the same cause, thus amplifying the effect and attracting the attention of the Government and media alike.

The first of such movements, the Arab Spring, optimistically demonstrated to the public that it is possible to bring down the dictators with just a social media account. A designated leader was deemed to be prone to behind-the-door deals with the existing regimes and corruption. Such leaderless, mass movements were fairly successful at that time, and overthrew dictators in Tunisia, Libya, Egypt, Yemen, Syria, and Bahrain[56].

Closer to home, there was the protest against the acquittal of Jessica Lal murder accused which led to the Delhi High Court taking cognizance suo motu and bringing the murderer to justice. There were also the protests for Nirbhaya, a grotesque and inhumane gang rape victim, that brought about speedy Presidential ordinances for amedments to the S.375 (which deals with rape) of the Indian Penal Code, which were ratified by the Parliament[57].

#MeToo was a movement for sexual harassment of women, which started as an anonymous blog post in 2017 that brought about the awareness and started the conversation against sexual harassments and assaults in the public domain[58]. In 2020, the Black Lives Matter movement

[56] Noah Tesch, *Arab Spring: Pro-Democracy Protests*, ENCYCLOPEDIA BRITANNICA, (Sept 7, 2011), https://www.britannica.com/event/Arab-Spring.
[57] Garima Bakshi, *The 'Nirbhaya' Movement: An Indian Feminist Revolution*, GNOVIS, (May 2, 2017), http://www.gnovisjournal.org/2017/05/02/the-nirbhaya-movement-an-indian-feminist-revolution/.
[58] Anon, *Understanding the Me Too Movement: A Sexual Harassment Awareness Guide*, MARYVILLE

brought about some serious conversations against racism and police brutality. Some of the oldest statues of colonial figureheads were brought down, names of the institutions were changed, historical accounts were corrected in cases of the aristocrats and prominent figures who took an active or passive role in the slave trade and racism[59].

XV. HUMANITARIAN CRISES: THE FLIP SIDE OF THE COIN

Humanitarian crises such as genocides, mass exodus, hate crimes have emerged in parallel to that of civilisations. Social media is the rose that comes with its share of thorns. Just like it amplifies revolutions, it amplifies the crises.

The Arab Spring destabilized the entire Middle East region. It led to some of the most brutal bombings in the history of mankind of the region by the "Peace Keeping" forces of the world- NATO, US and EU. Together with ongoing war in Iraq, Afghanistan, the trade sanctions against Iran, the entire region has been ravaged with wars, destruction of habitats and infrastructure, famines and lack of public healthcare. This has led to a severe famine and malnourishment where people, especially the children have turned into living skeletons. In turn, this resulted in mass exodus of populations and the severe refugee crisis in the EU where people cross the Mediterranean Sea at night in lifeboats filled more than three times their respective capacities[60].

In the Indian subcontinent, we have the Rohingya crisis, triggered by the terror attack by the Rohingya Extremist Group. In August 2017, Rohingyas started fleeing crackdown by the Myanmar Army. Reportedly, half a million Rohingya refugees are fleeing persecution after their homes and villages were burnt down. These events coincide with the rise in the internet users in Myanmar. The numbers tell us that the users have increased from 3 million to 30 million in a short span, from 2015 to 2020. There exist various Facebook groups promoting hate speech, violence against Rohingyas and has come under severe backlash internationally for not enforcing strict norms against hate speech[61].

XVI. DATA SURVEILLANCE: BYPASSING THE ENCRYPTION

Pegasus first came into the public eye in 2019. It was exposed by the Citizens Lab, based out

UNIVESITY BLOG, https://online.maryville.edu/blog/understanding-the-me-too-movement-a-sexual-harassment-awareness-guide/.

[59] Brian Duignan, *Black Lives Matter: International Activist Movement*, ENCYCLOPEDIA BRITANNICA, (Aug 13, 2020), https://www.britannica.com/topic/Black-Lives-Matter.

[60] Noah Tesch, *Arab Spring: Pro-Democracy Protests*, ENCYCLOPEDIA BRITANNICA, (Sept 7, 2011), https://www.britannica.com/event/Arab-Spring.

[61] Anon, *Myanmar Rohingya: What you need to know about the crisis*, BBC NEWS, (Jan 23, 2020), https://www.bbc.com/news/world-asia-41566561.

 [ISSN 2581-5369]

of Toronto. It was reportedly engaged in spying on 1,400 individuals around the world in 45 nations. Pegasus is a spyware designed and developed by an Israel based company- NSO Group (Niv, Shalev, Omri). It was revealed that it can be installed in the target's phone by sending them a clickbait link, phone calls/SMS from unknown numbers. Spyware gets access to all the phone calls, IMs, emails, photos, videos, locations, etc[62].

Pegasus was first detected in Saudi Arabia. It received its current infamy because it was found that it was used to spy on Jamal Khashoggi, a Saudi journalist and dissident who was later murdered in Saudi Arabian consulate in Istanbul. NSO claims that it sells the spyware exclusively to authorized government agencies. Pegasus has been used to target activists, journalists, human rights organizations, etc. It has been allegedly used by Middle East governments as well as India[63].

Pegasus is akin to the Orwellian Big Brother who had access to every personal detail as well as thoughts and behaviours from behind the screen installed in every living space, in this instance, our smartphones which have invaded our everyday lives.

XVII. PANDEMIC AND SURVEILLANCE

With SARS-CoV-2 virus raging around the world and causing COVID-19 pandemic, the Governments around the world have been encouraging the download of health surveillance apps. The highly infectious virus has been known to infect individuals in the briefest of contact with an infected carrier. In light of this, Governments developed apps that work on feedback mechanisms and allow people to see how many people are infected in the vicinity and how much is the distance between you and the said people, since a minimum 6 feet of social distance is advisable.

The surveillance apps are mandatory on the individuals that are infected, or have been contact-traced to an infected person, or who travel out of the city/state/country. One such app in India is Aarogya Setu. It had a whopping 100 million downloads in the first week of release. The app has access to all the personal data of the users. It consists of a live tracking feature using GPS and Bluetooth.The main criticism is that the app does not have an open source code, which can then be scrutinized by the developers around the world for bugs, and hence, can give backdoor entry to spyware. Life span of data storage is 180 days, however, there is no way to check if it

[62] Patrick Howell O'Neill, *Inside NSO, Israel's billion-dollar spyware giant*, MIT TECHNOLOGY REVIEW, (Aug 19, 2020), https://www.technologyreview.com/2020/08/19/1006458/nso-spyware-controversy-pegasus-human-rights/
[63] Ibid.

is deleted[64].

Not so surprisingly, the liability clause in user agreement frees the Government of all liabilities, in case of a data breach and its consequences[65].

XVIII. DATA PROTECTION LAWS

It is an opinion of human rights and data privacy activists that privacy is a fundamental right essential to human existence. One has a right to self-determination in a democratic system, without the manipulation by any kind of authority or organisations or people holding a position of power and/or influence.

One of the most progressive legislations for data protection is the General Data Protection Regulations, 2016.

(A) General Data Protection Regulations, 2016

In light of the above discussed events, a need for a comprehensive framework for data protection in line with the advancing technologies and personal liberty was felt. General Data Protection Regulations were developed and brought into force by the European Union in 2016. What sets GDPR apart is the principles enacted in the articles.

Article 5(1) sets down the 7 principles which must be honoured at all instances in the EU countries adopting GDPR. These are-

"(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary

[64] Andrew Clarance, *Aarogya Setu: Why India's Covid-19 contact tracing app is controversial*, BBC NEWS, (May 14, 2020), https://www.bbc.com/news/world-asia-india-52659520.
[65] Ibid.

 [ISSN 2581-5369]

for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

Further, Article 5(2) states that, "The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."

The GDPR provides the following rights for individuals:

1. The right to be informed (Art. 12, 13, 14)- Prior to the data collection, a data subject has the right to know the methods employed for collection, processing, and storage of the data, and the purposes of the same.
2. The right of access (Art. 12,15)- After the data collection, a data subject has the right to know the methods employed for collection, processing, and storage, the particulars of the data, and the purposes of the same.
3. The right to rectification (Art. 12,16)- This enables the data subject to correct the incorrect data, and to complete the data in case it is incomplete.
4. The right to erasure (Art. 12,17)- Also known as the "Right to be Forgotten", a data subject has the right to demand permanent deletion of his stored data.
5. The right to restrict processing (Art. 12, 18)- This gives the data subject the right to limit, control, or block any amount of personal data from processing
6. The right to data portability (Art. 12, 20)- "A data subject has the right to move, copy, or transfer personal data from one data controller to another, in a safe and secure way, in a commonly used and machine-readable format.

   Wherever technically possible, this also includes the right to have the data transferred directly from one controller to another without the data subject having to handle the data."
7. The right to object to processing (Art. 12,21)- This grants the right to object to any processing done by the private companies, authorities for profiling purposes or

 [ISSN 2581-5369]

otherwise, without the data subject consenting to it explicitly. It also grants the right to object to any inclusion in the databases for the purpose of marketing.

8. Rights in relation to automated decision making and profiling (Art. 12,22)- Perhaps the most important and remarkable right granted, the subjects have the right to demand a human intervention in the data processing and to not leave it solely to the algorithm's design and decision making process.

It must be noted that the GDPR, unlike many legislations around the world, uses a fairly simple, self-explanatory language which enables a layman to understand what it entails. As a result, a simple reading would educate the reader about the objective of the law, the functions and their rights.

(B) Personal Data Protection Bill, 2019

The PDP Bill in India has sought to codify and regulate the in which it didn't have a specific legislation solely dedicated to data prior to this. Like GDPR, it mainly defines data principal (data subject in GDPR), data fiduciary (organisations that collect, process, and store the data), data transport and data localisation.

1. Key Provisions:

1. Exemptions have been granted for the data collection, storage, and processing without the consent of the individual for "reasonable purposes". These include national security, tracking suspicious and unlawful activities, whistleblowers, emergencies, scoring the credit, search engine operations and processing of data on a public domain.
2. The Bill provides for an independent authority to regulate the data.
3. Every company will have to comply with the requirement of appointing a Data Protection Officer (DPO) who will liaison with the Data Protection Authority for the purpose of audits, redressal of grievances, maintenance of the records, etc.
4. The Bill has proposed "Purpose limitation" as well as "Collection limitation" clauses, akin to the said clauses in GDPR.
5. Data portability rights have been granted to the individuals to access and transfer one's own data.
6. Right to be Forgotten has also been granted, keeping in line with GDPR, allowing the consent for data collection and disclosure to be removed by the individual.

 [ISSN 2581-5369]

7. The Bill also provides for penalties in case of non-compliance. Rs 5 crore or 2 percent of worldwide turnover for minor violations and Rs 15 crore or 4 percent of total worldwide turnover for more serious violations. Also, the company's executives, who are in charge, can face imprisonment upto 3 years.

2. Advantages

1. Localization of data will assist authorities to obtain forensic and enforcement data.
2. Many of the cross-border data sharing is as of now, controlled by national bilateral arrangements on reciprocal legal assistance. It is a tedious procedure to access data via this path.
3. Cyber threats and monitoring events will be reviewed.
4. The use of social media for spreading misinformation, fake news and hate speeches, which lead to hate crimes, can be tracked and prevented.
5. Data localization would also improve the Government's ability to tax Internet moguls for all the financial transactions engaged into.

3. Disadvantages

1. Some argue that in the cyber world, the location of data in a physical sense is not important. The encryption and decryption solutions can still be beyond the purview of authorities even though the data is kept in the region.
2. An open-ended concept of "national defense" or "reasonable purposes" may contribute to the interference of the state into peoples' private lives.
3. The protectionist regime suppresses the ideals of a globalized, dynamic internet marketplace, where knowledge flows are dictated by prices and speeds instead of nationalist boundaries as stated by the tech giants like Facebook, Google.
4. It can also prove to be a disadvantage for India's own young start-ups attempting to expand internationally, or on companies handling international data in India due to the open ended data acquisition clause for nation defence, and the data localisation requirements.

XIX. CONCLUSION

It is clear that data has surpassed oil in terms of the value to the companies. Governments, too, have quickly picked up on the influence it can exert, and bend the opinion of people due to the access of personal data and psychoanalytic tools and algorithms. Surveillance capitalism has

 [ISSN 2581-5369]

arrived and very few people are questioning its legitimacy. Companies influence the market and economic behaviour of the users while the Governments influence the elections and crush the dissent by manipulating masses to an extent where they lose their ability to hold their Government accountable.

As of November 2019, Twitter showed its resolution to combat misuse of the platform by the Governments and banned political advertising on its platform. Further, during US Elections of November 2020 including the Presidential Election, Twitter flagged several tweets of President Donald Trump for misinformation and attached a link to a credible source. Further, the tweets which were deemed blatant lies and hate speech were hidden and had a disclaimer that stated so.

Awareness campaigns about data privacy and the consequence of its *ultra vires* and malicious use are the need of the hour. At the same time, it must be objectively understood that there are many forces on the internet constantly trying to break one's back and make them bend to their will. Hence, any piece of information, even if it comes from a source of repute must be fact checked and taken with a pinch of salt.

Steps must be taken by the individual to safeguard their data, suo motu, which translates into reading the terms and conditions, privacy policies before signing up for anything on the internet, taking the effort to read what "Accept all cookies" entail and more often than not, customising the cookie settings to make it less risky for personal usage.

*****

 [ISSN 2581-5369]

XX. BIBLIOGRAPHY

(A) Books

1. Richardson M., (2017). The Right to Privacy: Origins and Influence of a Nineteenth-Century Idea. Cambridge University Press.
2. Rule J. B., (2007). Privacy in Peril. Oxford University Press.
3. Floridi L., (2014). Protection of Information and the Right to Privacy - A New Equilibrium? Springer International Publishing.
4. Lyon D., (2003). Surveillance as Social Sorting. Routledge.
5. Voigt P. & Bussche A. V. D., (2017). The EU General Data Protection Regulation (GDPR). Springer International Publishing.
6. Khera R., (2019). Dissent on Aadhar: Big data meets Big Brother. Orient Blackswan.
7. Aiyar S., (2017). A Biometric History of India's 12-Digit Revolution. Westland Publication Ltd.

(B) Articles

1. Ashok Kumar Kasaudhan, *Surveillance and right to privacy: Issues and challenges*, Vol. 3, INT. JOURNAL OF LAW 73, 75 (2017).
2. Dr. Keith Goldstein et al, *Right to Privacy in the Digital Age*, OHCHR (April 9, 2018) https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/PiratePartiesInternational.pdf.
3. Priyanka Mittal, *Is privacy a fundamental right? Two cases that SC will look at*, LIVEMINT, (19 July 2017), https://www.livemint.com/Politics/7oHGx6UJfLD0uIDXFwV9CL/Is-privacy-a-fundamental-right-Two-cases-that-Supreme-Court.html
4. Bharat Vasani et al, *Right to Privacy: Surveillance in the post-Puttaswamy Era*, BLOOMBERG QUINT, (12 Nov 2019) https://www.bloombergquint.com/law-and-policy/right-to-privacy-surveillance-in-the-post-puttaswamy-era
5. *Watch the watchman series Part 2: Centralised Monitoring System*, INTERNET FREEDOM FOUNDATION, (14 Sept 2020) https://internetfreedom.in/watch-the-watchmen-series-part-2-the-centralised-monitoring-system/
6. *NETRA: A vigilant eye on the internet*, RESEARCH MATTERS, (8 Mar 2017) https://researchmatters.in/article/netra-vigilant-eye-internet

 [ISSN 2581-5369]

7. Paul Mozur, *Baidu and Cloudfare Boost Users over China's Great Firewall*, NYTIMES, (13 Sept 2015) https://www.nytimes.com/2015/09/14/business/partnership-boosts-users-over-chinas-great-firewall.html

8. Simon Denyer, *China's scary lesson to the world: Censoring the Internet works*, WASHINGTON POST, (23 May 2016) https://www.washingtonpost.com/world/asia_pacific/chinas-scary-lesson-to-the-world-censoring-the-internet-works/2016/05/23/413afe78-fff3-11e5-8bb1-f124a43f84dc_story.html

9. Chris Hoffman, *How the "Great Firewall of China" works to censor China's Internet*, HOW-TO GEEK, (10 Sept, 2017) https://www.howtogeek.com/162092/htg-explains-how-the-great-firewall-of-china-works/

10. Chris Brook, *What is Deep Packet Inspection? How it works, Uses cases for DPI, and more,* DIGITAL GUARDIAN, (5 Dec 2018) https://digitalguardian.com/blog/what-deep-packet-inspection-how-it-works-use-cases-dpi-and-more

11. Benjamin Haas, *China bans Winnie the Pooh film after comparisons to President Xi*, THE GUARDIAN, (7 Aug 2018), https://www.theguardian.com/world/2018/aug/07/china-bans-winnie-the-pooh-film-to-stop-comparisons-to-president-xi

12. Thomas J Ackermann, *What is china's SKYNET (yes: it is what you think it is)*, BGP4, (10 May 2019) https://www.bgp4.com/2019/05/10/what-is-chinas-skynet-yes-it-is-what-you-think-it-is/

13. Alfred Ng, *How China uses facial recognition to control human behaviour*, CNET, (11 August 2020) https://www.cnet.com/news/in-china-facial-recognition-public-shaming-and-control-go-hand-in-hand/

14. Paul Mozur, *Inside China's Dystopian Dreams: AI, Shame and Lots of cameras*, NY TIMES, (8 July 2018) https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html

15. Alexandra Ma, *China ranks citizens with a social credit system- Here's what you can do wrong and how you can be punished*, INDEPENDANT, (8 May 2018), https://www.independent.co.uk/life-style/gadgets-and-tech/china-social-credit-system-punishments-rewards-explained-a8297486.html

16. Ashley Gorski et al, *The future of US Foreign Intelligence Surveillance*, JUST SECURITY, (11 Nov, 2020) https://www.justsecurity.org/73321/the-future-of-u-s-foreign-intelligence-surveillance/

17. Bill Chappell, *NSA Reportedly Mines servers of US Internet firms for data*, NPR, (6 Jun 2013) https://www.npr.org/sections/thetwo-way/2013/06/06/189321612/nsa-reportedly-mines-servers-of-u-s-internet-firms-for-data

18. Andy Green, *Complete Guide to privacy Laws in the US*, VARONIS, (29 Mar 2020) https://www.varonis.com/blog/us-privacy-laws/

19. Evans Andrews, *Who Invented the Internet?*, HISTORY, (Oct 28, 2019), https://www.history.com/news/who-invented-the-internet/.

20. *Facebook Unveils Facebook Ads*, FACEBOOK, (Nov 6, 2007), https://about.fb.com/news/2007/11/facebook-unveils-facebook-ads/.

21. Josh Constine, *Twitter Ads Are Finally Available To All US Businesses, No Longer Invite Only*, TECH CRUNCH, (Apr 30, 2013), https://techcrunch.com/2013/04/30/twitter-ads-available/.

22. Mansoor Iqbal, *Facebook Revenue and Usage Statistics (2020)*, BUSINESS OF APPS, (Oct 30, 2020), https://www.businessofapps.com/data/facebook-statistics/

23. Phil Gray, *The Rise of Intelligent Virtual Assistants*, INTERACTIONS, (Jun 1, 2016), https://www.interactions.com/blog/intelligent-virtual-assistant/rise-intelligent-virtual-assistants/

24. Jonathan Haidt & Tobias Rose-Stockwell, *Social Media is Warping Democracy*, THE ATLANTIC, (Dec 2109), https://www.theatlantic.com/magazine/archive/2019/12/social-media-democracy/600763/

25. Julia Carrie Wong, *The Cambridge Analytica Scandal Changed the World- but it Didn't Change Facebook*, THE GUARDIAN, (Mar 18, 2019), https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook.

26. Newley Purnell & Jeff Horwitz, *Facebook's Hate-Speech Rules Collide With Indian Politics*, THE WALL STREET JOURNAL, (Aug 14, 2020), https://www.wsj.com/articles/facebook-hate-speech-india-politics-muslim-hindu-modi-zuckerberg-11597423346.

27. Noah Tesch, *Arab Spring: Pro-Democracy Protests*, ENCYCLOPEDIA BRITANNICA, (Sept 7, 2011), https://www.britannica.com/event/Arab-Spring.

28. Garima Bakshi, *The 'Nirbhaya' Movement: An Indian Feminist Revolution*, GNOVIS, (May 2, 2017), http://www.gnovisjournal.org/2017/05/02/the-nirbhaya-movement-an-indian-feminist-revolution/

29. Anon, *Understanding the Me Too Movement: A Sexual Harassment Awareness Guide*, MARYVILLE UNIVESITY BLOG, https://online.maryville.edu/blog/understanding-the-me-too-movement-a-sexual-harassment-awareness-guide/.

30. Brian Duignan, *Black Lives Matter: International Activist Movement*, ENCYCLOPEDIA BRITANNICA, (Aug 13, 2020), https://www.britannica.com/topic/Black-Lives-Matter.

31. Anon, *Myanmar Rohingya: What you need to know about the crisis*, BBC NEWS, (Jan 23, 2020), https://www.bbc.com/news/world-asia-41566561.

32. Patrick Howell O'Neill, *Inside NSO, Israel's billion-dollar spyware giant*, MIT TECHNOLOGY REVIEW, (Aug 19, 2020), https://www.technologyreview.com/2020/08/19/1006458/nso-spyware-controversy-pegasus-human-rights/.

33. Andrew Clarance, *Aarogya Setu: Why India's Covid-19 contact tracing app is controversial*, BBC NEWS, (May 14, 2020), https://www.bbc.com/news/world-asia-india-52659520.

*****

 [ISSN 2581-5369]